PA252-en00

[19]中华人民共和国专利局

[51]Int.Cl[6]
G06F 12/14

[12] 发明专利申请公开说明书

[21] 申请号 96121967.X

[43]公开日 1997 年 7 月 16 日

[11] 公开号 CN 1154512A

[22]申请日 96.11.6

[30]优先权

[32]95.11.7 [33]JP[31]289009/95

[32]95.11.7 [33]JP[31]289011/95

[71]申请人 富士通株式会社

地址 日本神奈川

[72]发明人 片冈达史 吉冈诚
内海研一 村上敬一

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

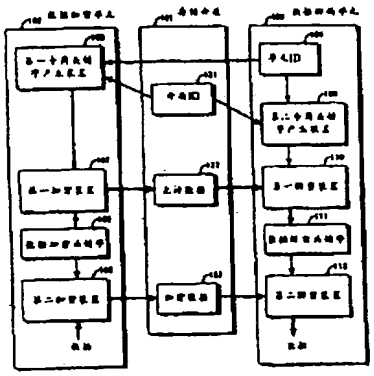
代理人 鄢 迅

权利要求书 3 页 说明书 11 页 附图页数 13 页

[54]发明名称 保护存储在便携式存储介质的信息的保密系统

[57]摘要

一种通过检查分配给每个介质、系统和终端的标识符保护存储在便携式存储介质中的信息的保密系统。数据以加密形式存储在介质上。保密系统在允许用户执行任何数据存取之前检查介质 ID、系统 ID 和终端 ID 的有效性，并对其进行管理，从而保护内容不被越权存取。保密系统也将允许数据写入每个存储介质来管理其中存储的加密数据的解密。允许数据包含解密该数据必须的加密关键字，并且仅能使用有效的介质 ID 和单元 ID 解码该关键字。



(BJ)第 1456 号

权 利 要 求 书

1．一种保护存储在存储介质的数据的保密系统，该保密系统包括：

预先写入该存储介质的单个标识符；

唯一分配给终端的终端标识符；和

仅当从所述的存储介质提取的所述的单个标识符和从终端提取所述的终端标识符两者都有效时用于允许该终端存取存储介质中的数据的保密控制装置。

2．根据权利要求1所述的保密系统，其中所述的保密控制装置处于终端之内。

3．根据权利要求1所述的保密系统，其中所述的保密控制装置是以终端的保密控制程序设置的。

4．根据权利要求1所述的保密系统，其中当所述的单个的标识符和所述的终端标识符两者都有效时加密或解密数据。

5．根据权利要求1所述的保密系统，其中当所述的单个的标识符、所述的终端标识符和用户标识符全部都有效时加密或解密数据。

6．根据权利要求1所述的保密系统，其中所述的单个的标识符是唯一分配给存储介质的介质标识符。

7．根据权利要求1所述的保密系统，其中所述的单个的标识符是唯一分配给计算机系统的系统标识符。

8．根据权利要求1所述的保密系统，仅当唯一分配给存储介质的介质标识符和从终端提取的所述的终端标识符两者都有效时才允许保密控制程序安装到该终端。

9．一种保护存储在存储介质中的信息的保密系统，包括：

便携式存储介质，用于存储信息，并具有唯一分配给它的介质标识符；和

计算机单元，具有单元标识符，用于读和写所述存储介质中的信息，包括：

第一加密装置，用于将允许数据以加密形式写入所述的存储介质，允许数据是通过使用从所述的存储介质提取的介质标识符、单元标识符以及数据加密关键字经加密产生的，

第二加密装置，用于使用数据加密关键字对数据加密并将加密数据写入存储介质，

第一解密装置，用于当所述的计算机单元企图检索写入所述存储介质的加密数据时，通过使用允许数据和从所述存储介质提取的介质标识符、以及单元标识符经解密产生数据解密关键字，和

第二解密装置，用于使用由所述的第一解密装置产生的数据解密关键字对从所述的存储介质提取的加密数据进行解密。

10．一种保护存储在存储介质中的信息的保密系统，包括：

便携式存储介质，用于存储信息，并具有唯一分配给它的介质标识符；和

计算机单元，具有一单元标识符，用于读和写所述的存储介质中的信息，包括：

第一专用关键字产生装置，用于当所述的计算机单元企图将数据写入所述的存储介质时，根据从所述的存储介质提取的介质标识符和单元标识符产生专用关键字，

第一加密装置，用于通过使用由所述的第一专用关键字产生装置产生的专用关键字对数据加密关键字进行加密来产生允许数据，并将允许数据写入所述的存储介质，

第二加密装置，用于使用数据加密关键字对数据进行加密，并将加密数据写入存储介质，

第二专用关键字产生装置，用于当所述的计算机单元企图检索写入所述的存储介质中的加密数据时，根据从所述存储介质提取的介质标识符和单元标识符再次产生专用关键字，

第一解密装置，用于通过使用由所述的第二专用关键字产生装置再次产生的专用关键字对从所述的存储介质提取的允许数据进行解密来产生数据解密关键字，和

第二解密装置，用于使用由所述的第一解密装置产生的数据解密关键字对从所述的存储介质提取的加密数据进行解密。

11．根据权利要求9所述的保密系统，其中所述的第一加密装置产生对应于分配给不同的保密控制单元的不同的单元ID的多个允许数据，并将多个允许数据写入所述的存储介质。

12．根据权利要求9所述的保密系统，其中所述的第一加密装置产生对应于被加密的不同数据的多个允许数据并将多个允许数据写入所述的存储介质。

13．根据权利要求9所述的保密系统，其中单元标识符被唯一分配给所述的计算机单元。

14．根据权利要求9所述的保密系统，其中单元标识符被唯一分配给用于读和写所述存储介质的便携式驱动单元。

说 明 书

保护存储在便携式存储介质的信息的保密系统

本发明涉及保护存储在便携式存储介质的信息的保密系统。尤其涉及，通过确认写入存储介质的标识符保护存储在便携式存储介质的信息的保密系统。本发明也涉及通过使用密码术保护存储在便携式存储介质的数据的保密系统。

现在的海量存储设备技术允许大量信息存入便携式存储介质，并且新的大容量介质，例如磁－光（MO）盘，用于在脱机基础上传输数据和程序。在经通信网络把多个终端连接到主计算机的商业计算机系统中，每个终端的执行程序，和日常作业中处理的数据，存储在这些便携式存储介质并从总站传送到终端，反之亦然。除能够存储大容量文件之外，它们易于携带，存放，和使用。

然而，在商业活动中，由于数据文件内容的保密特点数据保密将是一个严重的问题。因为如此重要的存储介质一直存在着可能丢失或在运输中被窃取的危险，所以通常使用口令保护技术保护介质中的信息免受越权存取并保证可靠地传送。预先将一个口令，或唯一定义的标识符，写入存储介质，并且要求企图存取存储介质内容的用户输入正确的口令。

这种传统的口令保护是简单的并且易于实现，但是应该注意到这样的口令也是窃取者和非法使用者所研究的潜在的问题。特别在数据和用于检索的程序密封在同一介质的情况下，数据将遭受更大的被窃取的危险和威胁，因为任何终端设备都能用于检索该数据。因此，一直存在对于保护存储介质中的信息不被越权存取并且保证安全地传输的更加可靠的保密系统的需求。

基于上面的考虑，本发明的一个目的是提供用于保护存储在便携式存储介质中的信息以保证安全传输的可靠的保密系统。

本发明的另一目的是提供用于通过仅允许限定的终端检索并解码加密数据来保护加密和存储在便携式存储介质中的数据的可靠的保密系统。

为实现上述的目的，根据本发明，提供保护存储在存储介质中的数据的保密系统。这种保密系统包括一个单个标识符、终端标识符和保密控制装置。

单个标识符是一个预先写入存储介质的标识符。终端标识符是唯一分配给该终端的标识符。仅当从存储介质提取的单个标识符和从终端提取的终端标识符两者都是有效时，保密控制装置才允许该终端存取存储介质中的数据。

为实现上面的目的，提供保护存储在存储介质中的信息的另一保密系统。这种保密系统包括一存储介质和一保密控制单元。存储介质为存储信息的便携式介质。存储介质具有唯一分配给它的介质标识符。保密控制单元用于读取和写入存储介质中的信息，并且它具有唯一分配给它的单元标识符。

保密控制单元包括四个单元。当保密控制单元企图将数据写入存储介质时，第一专用关键字产生装置根据从存储介质提取的介质标识符和单元标识符产生一专用关键字。第一加密装置通过使用由第一专用关键字产生装置产生的专用关键字对数据加密关键字进行加密来产生允许数据，并且它将允许数据写入存储介质。第二加密装置使用数据加密关键字对数据进行加密，并将加密数据写入存储介质。当保密控制单元企图检索写入存储介质的加密数据时，第二专用关键字产生装置根据从存储介质提取的介质标识符和单元标识符再产生专用关键字。第一解密装置通过使用由第二专用关键字产生装置再次产生的专用关键字对从存储介质提取的允许数据进行解密来产生数据解密关键字。第二解密装置使用由第一解密装置产生的数据解密关键字对从存储介质提取的加密数据进行解密。

通过对于以实例方式说明本发明的优选实施例并结合附图所进行的下面的描述，本发明的上面和其它目的，特点和优点将更明显。

图 1 是表示在本发明的第一实施例中使用加密系统的计算机系统的结构图，

图 2 是表示特许存储介质的过程的流程图；

图 3 是表示特许表的图；

图 4 是表示记录在包括加密控制信息的存贮介质中的数据的图；

图 5 是表示限定终端的过程的流程图；

图 6 是表示将数据写入存储介质的过程的流程图；

图 7 是表示从存储介质读出数据的过程的流程图；

图 8 是表示将保密控制程序安装到终端的过程的流程图；

图 9 是表示在本发明的第二实施例中的保密系统的结构图；

图 1 0（A）和 1 0（B）是表示记录在存储介质的信息的结构图；

图 1 1 是表示加密主观数据的过程的流程图；

图 1 2 是表示产生允许数据的过程的流程图；和

图 1 3 是表示对存储的数据进行解密的过程的流程图；

下面参考附图描述本发明的两个实施例。

首先，参考图 1 到 8 将描述第一实施例。

图 1 表示本发明的第一实施例中使用保密系统的计算机系统的全部结构。例如，在这种提供银行服务的商业计算机系统中，位于总部 1 的主计算机 2 具有多个本地终端。经数据通信网，主计算机 2 连接到公司的支局 1 0，在这里设置多个终端。这些本地和远程终端 1 1 的控制集中在主计算机 2，在这里特许表 3 提供限定系统管理者和使用者的信息。

每个终端 1 1 与主计算机 2 通信来执行商业业务，并通过驱动单元 4 从存储介质 5 读取数据和写入数据到存储介质 5。保密控制器 1 2 控制对内容的存取，和监视当数据写入存储介质 5 时执行的数据加密处理。

存储介质 5 与后面将描述的一些保密控制信息一起，以加密形式存储数据和程序。磁－光（MO）盘和其他的可重写便携式介质适用于存储介质 5。驱动单元 4 是用于写入和读出这种存储介质 5 中的数据的硬件设备。

下面的描述将详细解释第一实施例的保密系统的有关操作。

图 2 是表示特许存储介质的过程的流程图。在本发明中，每个存储介质 5 被初始化以便包含一些保密信息。该过程采取下面的 4 个步骤：

[S 1] 使用激光束以永久方式将唯一的介质标识符（ＩＤ）写入或烧灼到存储介质 5（例如，ＭＯ盘）的非重写区。在装运之前通过存储介质 5 的制造者完成步骤Ｓ 1。永久介质ＩＤ使得不易伪造存储介质 5。

[S 2] 参考特许表 3，保密控制器 1 2 检查是否输入正确的管理者的口令。例如，当总部 1 的操作员已经将一新介质插入终端 1 1 的驱动单元 4 时，保密控制器 1 2 将要求他/她输入用户ＩＤ和口令。如果在特许表 3 发现输入的口令为对初始化介质有控制权的特许管理者，该过程进到下一步骤　Ｓ 3。否则，终止过程。

[S 3] 既然认可操作者，保密控制器 1 2 确定唯一ＩＤ来识别其中存储介质 5 能运行的计算机系统。这种企业－特定的标识符认为是系统ＩＤ或企业ＩＤ。例如，选择“Ｂａｎｋ　ＡＡＡ”作为企业ＩＤ就是出于这个目的。

[S 4] 将在步骤Ｓ 3 确定的系统ＩＤ（企业ＩＤ）写入存储介质 5，然后初始化用于终端ＩＤ和加密数据（后面描述的）的其他数据区。

通过上述的过程，存储介质 5 已获得适当的格式，作为将来在特定公司的支局使用的“特许介质”。

图 3 表示本发明实施例中使用的特许表 3。特许表 3 的每一项目包含用户ＩＤ，用户分类，口令，等等，它们预先被登记。用户分类数据通过将用户分类为系统管理者，一般用户，及其他用户来限定用户，并定义他们的作业责任及对于存储数据的存取权。在图 2 的流程图中的步骤Ｓ 2，保密系统查阅这种特许表 3 以检索用户限定数据和对应于用户输入的用户ＩＤ的注册口令。如果检索的用户限定数据表示该用户是一个管理者，并且如果输入的口令与注册口令一致，用户将被允许进入产生特许存储介质的步骤Ｓ 3 和Ｓ 4。

图 4 表示记录在存储介质的示范的数据包括保密控制信息，例如，该数据包括下面的信息：

· 介质ＩＤ
· 企业ＩＤ

· 终端ＩＤ

· 加密数据

· 其他数据

如上所述，介质ＩＤ为由制造者唯一分配给每个介质的标识符。企业ＩＤ为通过公司操作计算机系统写入的标识符。终端ＩＤ为用于将存储介质用于特定终端的可选标识符。该终端ＩＤ使有指定终端ＩＤ的终端具有读取和写入该存储介质的特权。

图５是表示通过给出上述的终端ＩＤ将存储介质与特定的终端相联系的过程的流程图。该进程采用下面的两个步骤。

[Ｓ１１] 支局的管理员确定唯一被允许读取和写入该介质的特定终端的标识符。使用其单元号可以唯一识别支局的每个终端，能够使用单元号作为终端ＩＤ。在步骤Ｓ１１，保密系统接受由管理员确定的终端ＩＤ。

[Ｓ１２] 将终端ＩＤ写入特许存储介质，从而给出该终端专用的读/写存取特权。

通过上述的过程，从总部１传输的特许存储介质已获得终端ＩＤ，以便其内容仅对于由检查ＩＤ一致所限定的特定终端是可存取的。企业ＩＤ也用于限定处理存储介质的计算机系统。

图６是表示将数据写入特许存储介质的过程的流程图。假定总部１或者支局１１的其中之一的一个操作者现在企图将数据写入存储介质５。该过程采用下面的六个步骤。

[Ｓ２１] 操作者将存储介质５插入终端１１的其中之一的驱动单元４。

[Ｓ２２] 响应于存储介质５的插入，保密控制器１２通过搜索预定的只读区检查存储介质５是否包含介质ＩＤ。如果在这里发现有效的介质ＩＤ，因为它已经了解到该介质由合法的制造者制造，所以过程进入到下一步骤Ｓ２３。如果未发现有效的介质ＩＤ，将终止该过程，并怀疑存储介质５为非法的介质。

[Ｓ２３] 保密控制器１２检查存储介质５是否包含企业ＩＤ。如果发

现有效的企业ＩＤ，因为已经了解到存储介质５已在总部１进行适当处理，所以过程进入下一步骤Ｓ２４。如果未发现有效的企业ＩＤ，将终止该过程。

[Ｓ２４] 保密控制器１２检查该终端是否具有有效的存取权。尤其是，检查保密控制器１２或存储介质５中的终端ＩＤ是否与使用的终端的标识符一致。如果该终端具有有效的存取权，过程进入到下一步骤Ｓ２５。如果不是这样，将终止该过程。

[Ｓ２５] 在已知的诸如数据加密标准（ＤＥＳ）这样的数据加密算法下，加密主观数据。

[Ｓ２６] 将加密数据写入存储介质５。

通过上述的过程，仅在存储介质５具有正确的介质ＩＤ和企业ＩＤ以及终端具有对于存储介质５的有效的有效权的条件下，数据才能写入存储介质５。

接着，进行读出存储介质中的加密数据的过程。图７是表示在总部１或者支局１１其中之一的一个操作者，现在企图从存储介质５检索数据的情况下这种数据读出过程的流程图。该过程采用下面的八个步骤。

[Ｓ３１] 操作者将存储介质５插入终端１１的其中之一的驱动单元４。

[Ｓ３２] 响应于存储介质５的插入，保密控制器１２通过搜索预定的只－读区检查存储介质５是否包含介质ＩＤ。如果发现有效的介质ＩＤ，因为已经了解到由合法的制造者制造该介质，过程进入下一步骤Ｓ３３。如果未发现有效的介质ＩＤ，将终止该过程，并怀疑存储介质５为非法的介质。

[Ｓ３３] 保密控制器１２检查存储介质５是否包含企业ＩＤ。如果发现有效的企业ＩＤ，因为已经了解到在总部１已适当处理过该存储介质５，所以过程进入下一步骤Ｓ３４。如果未发现有效的企业ＩＤ，将终止该过程。

[Ｓ３４] 保密控制器１２检查终端是否具有有效的存取权。尤其是，检查保密控制器１２或者存储介质５中的终端ＩＤ是否与使用的终端的标

识符一致。如果该终端具有有效的存取权，过程进入步骤S 3 6。如果不是这样，过程进入步骤S 3 5。

[S 3 5] 通过总部1的系统管理者的有效口令可以补偿步骤S 3 4发现的终端ID的一致性的不足。步骤S 3 5测试是否输入这种管理者的口令。如果输入的口令是有效的，过程进入步骤S 3 6。如果未输入或者输入的口令无效，就终止该过程。

[S 3 6] 从存储介质5读出以加密形式存储的数据。

[S 3 7] 解密，或者加密该数据。

[S 3 8] 在终端的本地存储单元中存储解密数据。

保密控制器12实际上实现为每个终端执行的软件程序，该程序认为是保密控制程序。本发明对于这种重要的保密控制程序是提供保护。

图8是表示将保密控制程序安装到一终端的过程的流程图。该过程保护保密控制程序不在非授权终端安装或执行，这样就避免非法存取存储介质5的内容。该过程采用下面的四个步骤。

[S 4 1] 管理者的口令和企业ID写入保密控制程序的保留区。将使用具有这种附加保护信息的程序作为后面描述的“主程序”。

[S 4 2] 主程序的拷贝将分发到支局。

[S 4 3] 将所传送的保密控制程序安装到每个支局的每个终端。

[S 4 4] 在每个终端，将唯一的终端ID写入存储在终端中的本地存储单元的保密控制程序的另一保留区。

通过上述的过程，定做专用于该终端的保密控制程序；即，即使在其他终端被复制和安装，控制程序也不能工作。当启动时，保密控制程序比较其本身的终端ID和终端的实际ID，并且如果它们互相不一致就中断程序。

一旦每个终端安装和定做保密控制程序，其将来的再次安装也将受到限制。用于再次安装或者程序更新的存储介质，必须具有与使用的终端所指示的实际终端ID一致的终端ID注册。如果这种比较失败，将拒绝再次安装保密控制程序。

上述的第一实施例总结如下。根据本发明的保密系统，仅当存储介质

包含有效的介质ＩＤ、企业ＩＤ和终端ＩＤ时才允许存取存储介质（即，读或写存储其中的加密数据）。终端ＩＤ允许特定的终端以专用方式使用存储介质和保密控制程序。在介质ＩＤ，企业ＩＤ和终端ＩＤ所检测的任何不一致将中止读和写数据或安装程序的过程，这样就保护保密信息不被非法存取、窃取以及其他的危险和威胁。

接着，参考图９到１３下面将描述本发明的第二实施例，该实施例提供一种通过仅允许限定的终端搜索和解码已加密的数据来保护加密和存储在便携式存储介质中的数据的可靠的保密系统。

图９表示本发明的第二实施例的保密系统的结构。在图９中，存储介质　１０１是一个与包括唯一的介质ＩＤ和允许数据的一些保密控制信息一起存储加密数据的便携式海量存储介质。磁－光（ＭＯ）盘适用于存储介质５。

介质ＩＤ１２１是唯一地分配给存储介质１０１的标识符，例如，使用激光束以非－重写的方式在预定区域烧灼该标识符。这种永久的介质ＩＤ使得不易伪造存储介质１０１。允许数据１２２实际是使用专用关键字加密的数据加密关键字１０６。加密数据１２３是使用数据加密关键字１０６经诸如ＤＥＳ这样的数据加密算法加密的数据。

数据编码单元１０２包括第一专用关键字产生装置１０５，第一加密装置１０７和对数据以及加密关键字进行加密的第二加密装置１０８。

第一专用关键字产生装置１０５根据从存储介质１０１提取的介质ＩＤ１２１和单元ＩＤ１０４产生一专用关键字。单元ＩＤ１０４是计算机系统本身的或者便携式驱动单元（例如，ＭＯ驱动器）的唯一的标识符。虽然前一个标识符一般用作为单元ＩＤ１０４时，但是后一个在某些场合可能是有用的，例如系统安装或者维护，因为对于不同的计算机系统可能使用相同的驱动单元和存储介质来安装程序、建立数据，以及修改数据。第一加密装置１０７使用由第一专用关键字产生装置１０５产生的专用关键字对数据加密关键字１０６进行加密。将加密的加密关键字写入存储介质１０１作为前面提到的允许数据１２２。第二加密装置１０８使用数据加密关键字１０６对数据进行加密并将加密数据写入存储介质１０１作为

前面提到的加密数据１２３。

数据解码单元１０３包括第二专用关键字产生装置１０９、第一解密装置１１０和第二解密装置 112 从介质ＩＤ１２１、允许数据１２２和加密数据１２３中对数据进行解密。

第二专用关键字产生装置１０９根据从存储介质１０１提取的介质ＩＤ　１２１和单元ＩＤ１０４产生一专用关键字。为获得数据解密关键字１１１，第一解密装置１１０使用由第二专用关键字产生装置１０９产生的专用关键字对存储介质１０１中的允许数据１２２进行解密。第二解密装置１１２使用由第一解密装置１１０产生的数据解密关键字１１１对加密数据１２３进行解密。

图１０（Ａ）和１０（Ｂ）表示存储在存储介质１０１中的信息的结构。如图１０（Ａ）特定表示的，该信息包括：

· 介质ＩＤ
· 企业ＩＤ
· 允许数据＃１－＃ｎ
· 加密数据＃１－＃ｎ

如上所述，介质ＩＤ为使用激光束或类似物唯一烧灼到每个介质的标识符，ＩＤ防止介质被伪造。企业ＩＤ为唯一分配给每个公司以便相区分它们的计算机系统的标识符。允许数据＃１－＃ｎ和加密数据＃１－＃ｎ是为多个单元（ｎ个单元）准备的。当将相同数据组写入或将相同的程序安装到多个单元时，将ｎ组允许数据存储在存储介质１０１。在这种情况下，多个允许数据对应于单组解密数据。

图１０（Ｂ）示意地表示允许数据和单元ＩＤ之间的联系。从图９看出，允许数据１２２来自单元ＩＤ１０４和介质ＩＤ１２１，因此对于不同单元ＩＤ它具有不同的值。图１０（Ｂ）表示允许数据＃１，＃２，＃３等是如何对应于不同的单元ＩＤ＃１，＃１，＃３等的。

接着，参考图１１将详细描述产生加密数据１２３的过程。

图１１是表示加密存储数据的过程的流程图。该过程采用下面的四个步骤。

[S５１] 选择数据以便加密。

[S５２] 确定数据加密关键字１０６。

[S５３] 第二加密装置１０８使用数据加密关键字１０６加密选择的数据。

[S５４] 将加密数据１２３存储到存储介质１０１。

接着，参考图１２将详细描述产生允许数据１２２的过程。

图１２是表示产生允许数据１２２的过程的流程图。该过程采用下面的六个步骤。

[S６１] 第一专用关键字产生装置１０５从数据解码单元１０３提取单元ＩＤ１０４。

[S６２] 第一专用关键字产生装置１０５从存储介质１０１提取介质ＩＤ１２１。

[S６３]第一专用关键字产生装置１０５从分别在步骤Ｓ６１和Ｓ６２提取的单元ＩＤ１０４和介质ＩＤ１２１产生一专用关键字。

[S６４] 第一加密装置１０７ 使用专用关键字对数据解密关键字１０６进行加密来产生允许数据１２２。

[S６５] 将允许数据１２２存储到存储介质１０１。

[S６６] 测试是否已经处理全部可用的单元ＩＤ。如果完成全部的单元ＩＤ，就结束该过程。否则，该过程返回用于下一单元ＩＤ的步骤Ｓ６１。

最后，参考图１３下面将描述解密存储数据的过程。

图１３是表示解密加密数据１２３的过程的流程图。该过程采用下面的六个步骤。

[S７１] 第二专用关键字产生装置１０９提取数据解码单元１０３的单元ＩＤ１０４。

[S７２] 第二专用关键字产生装置１０９从存储介质１０１提取介质 ＩＤ１２１。

[S73] 第二专用关键字产生装置109从分别在步骤S71和S72提取的单元ID104和介质ID121产生一专用关键字。

[S74] 第一解密装置110使用专用关键字解密允许数据122来检索数据解密关键字111。

[S75] 第二解密装置112通过使用数据解密关键字111对数据进行解密来从加密数据123提取原始数据。

[S76] 测试是否已处理完全部可用的加密数据。如果完成全部数据，就结束该过程。否则，过程返回到用于下一数据的步骤S74。

上面的关于第二实施例的讨论总结如下。根据本发明，保密系统使用单元ID、介质ID和数据加密关键字不但加密原始数据而且加密其允许数据并将它们存入存储介质。只有具有相关单元ID的单元才能检索原始数据，这样就保护存储的数据不被非法存取。

上面仅就本发明的原理进行了说明。更进一步，因为本领域技术人员将很容易对其作出许多修改和变化，所以不应该将本发明限制到所表示和描述的准确的结构和应用，因此，全部适用的修改和等效物都认为是属于本发明附加权利要求书和它们的等效物的范围之内。

图 1

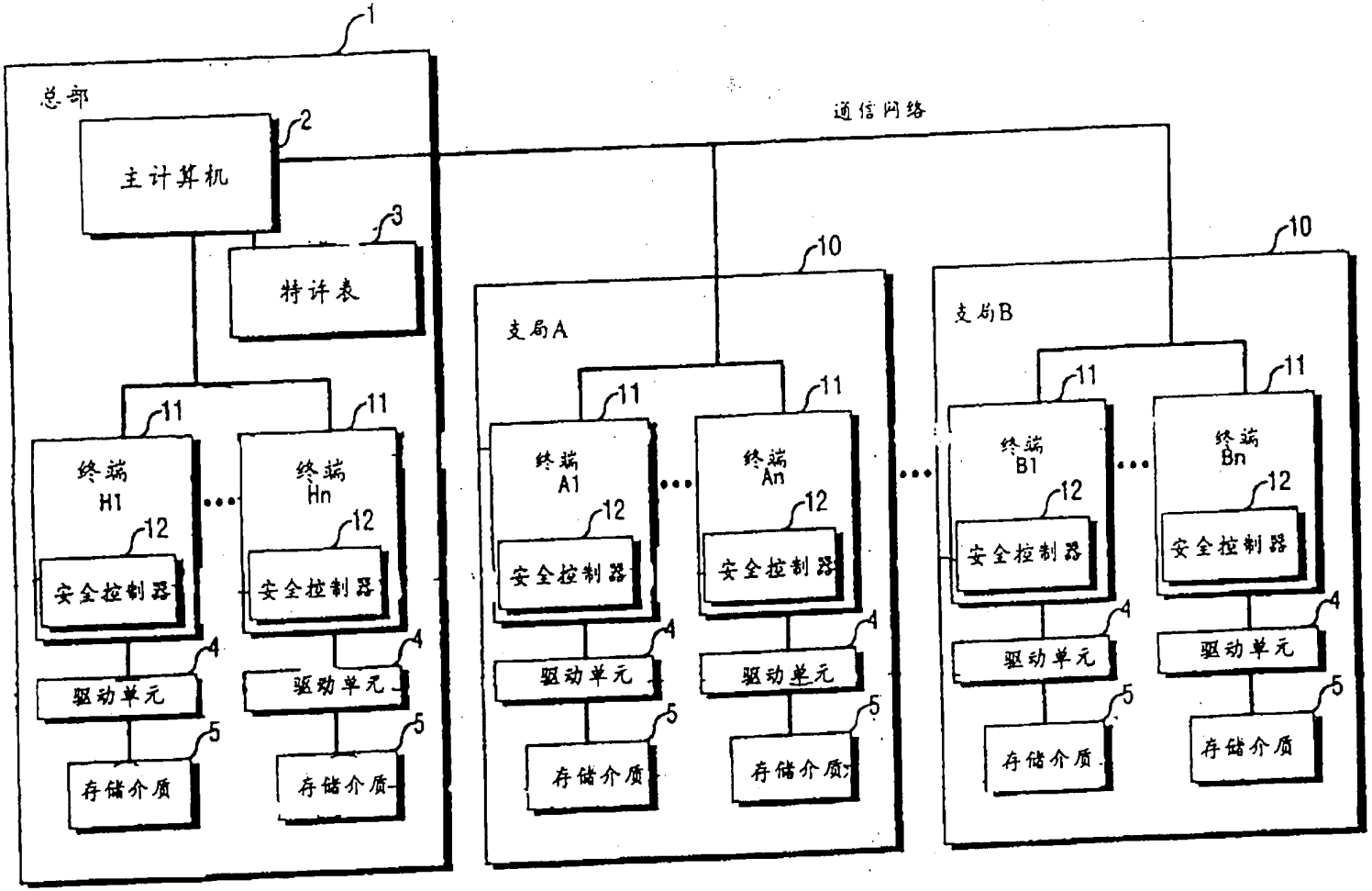


图 2

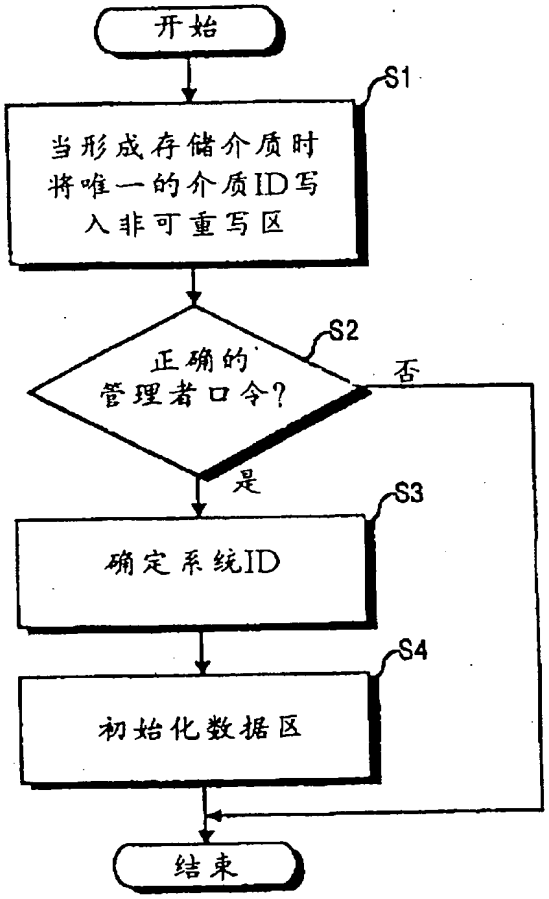

开始
S1
当形成存储介质时
将唯一的介质ID写
入非可重写区
S2
正确的
管理者口令?
否
是
S3
确定系统ID
S4
初始化数据区
结束

图 3

3

---	用户分类	口令	
aaaaaa	管理者	xxxxxx	
bbbbbb	一般用户	yyyyyy	
⋮	⋮	⋮	
⋮	⋮	⋮	

图 4

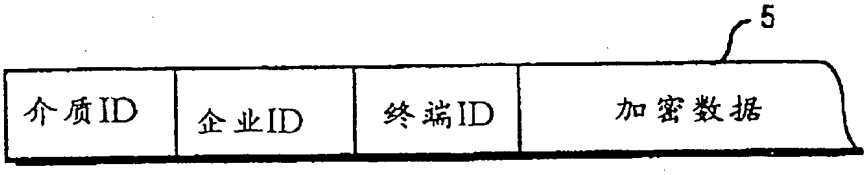


图 5

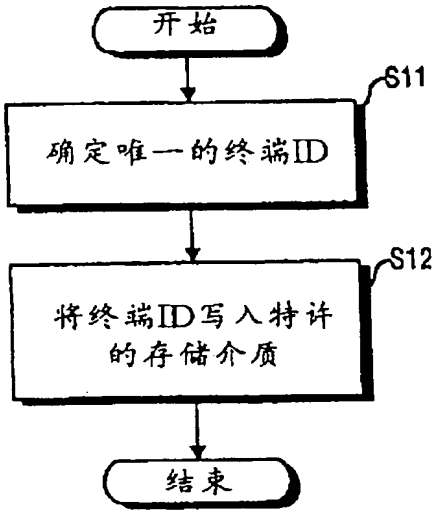


图 6

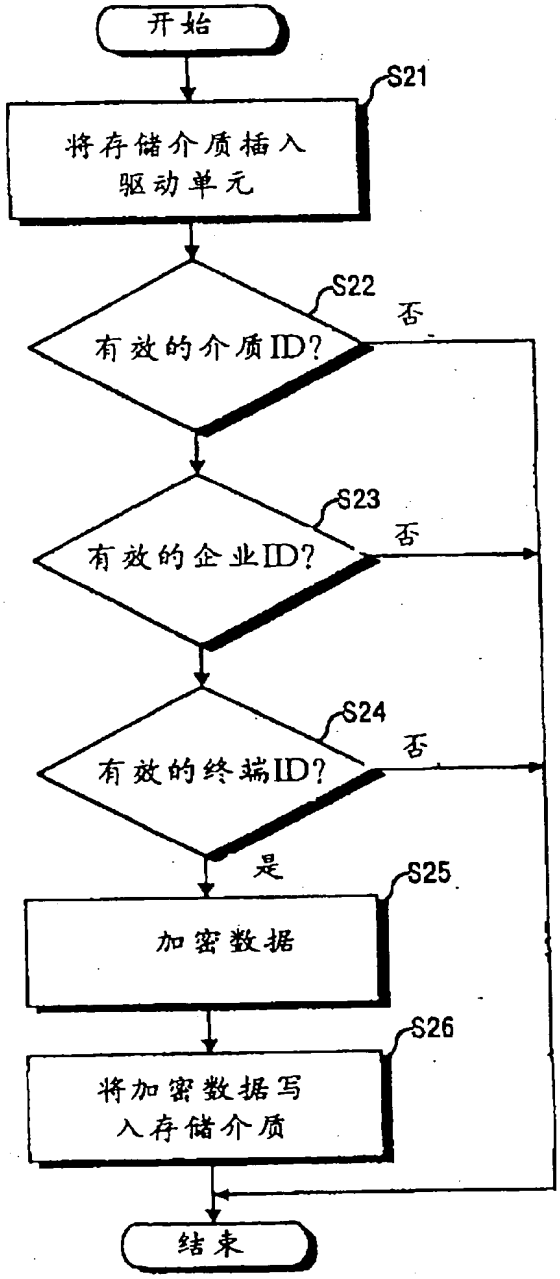

开始
S21
将存储介质插入驱动单元
S22
有效的介质ID?
否
S23
有效的企业ID?
否
S24
有效的终端ID?
否
是
S25
加密数据
S26
将加密数据写入存储介质
结束

图 7

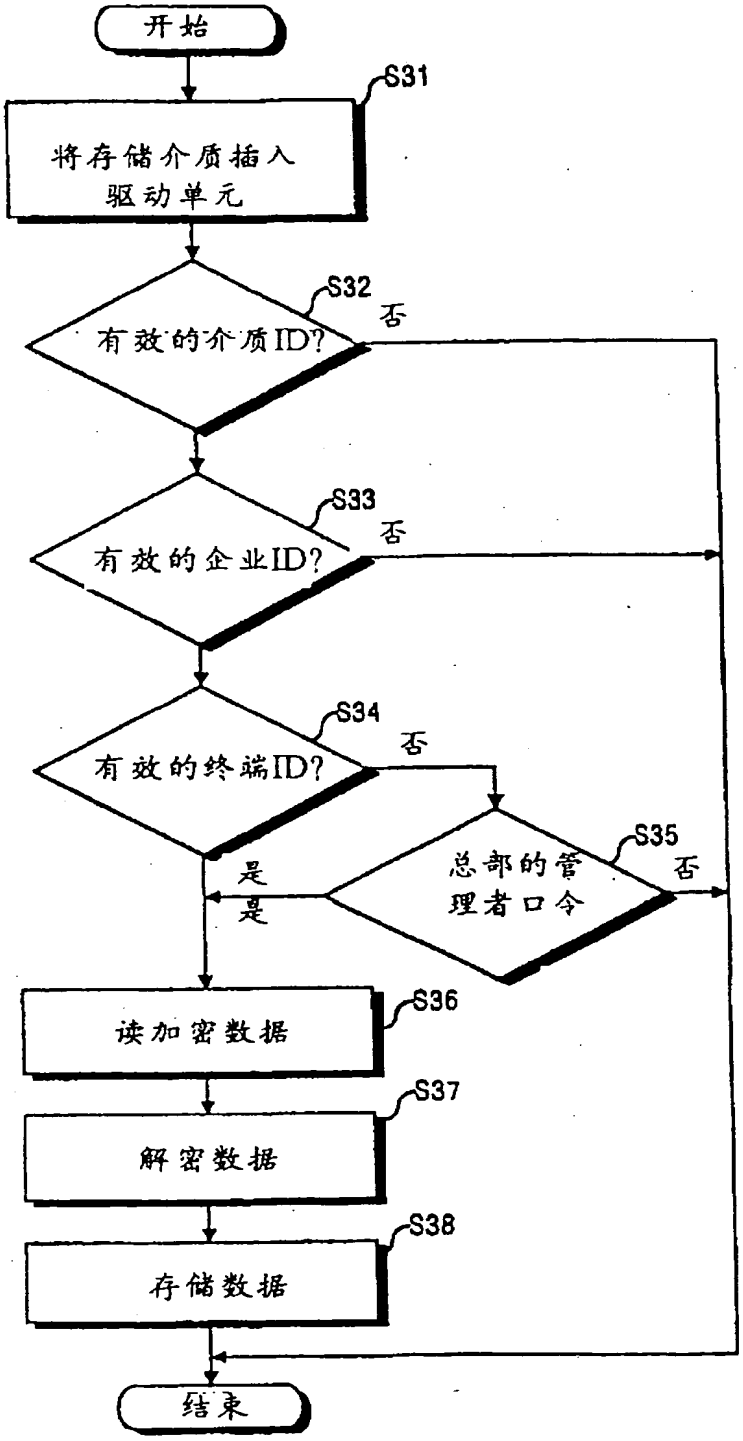


图 8

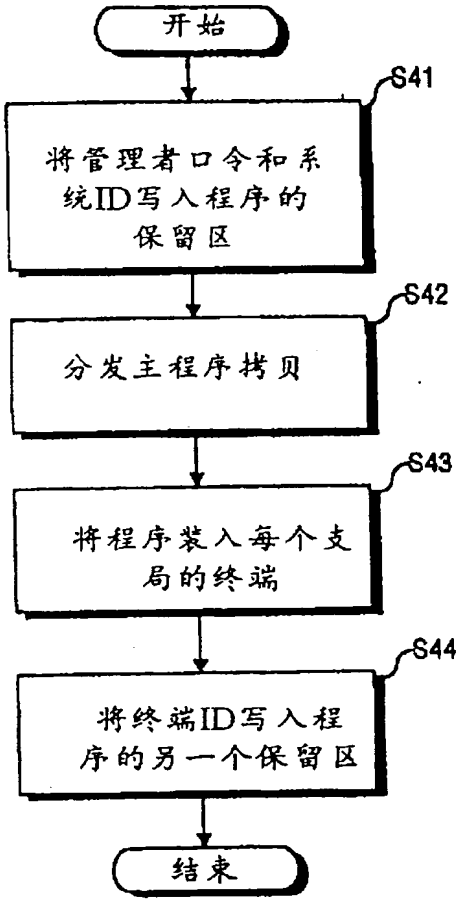

开始
S41
将管理者口令和系统ID写入程序的保留区
S42
分发主程序拷贝
S43
将程序装入每个支局的终端
S44
将终端ID写入程序的另一个保留区
结束

图 9

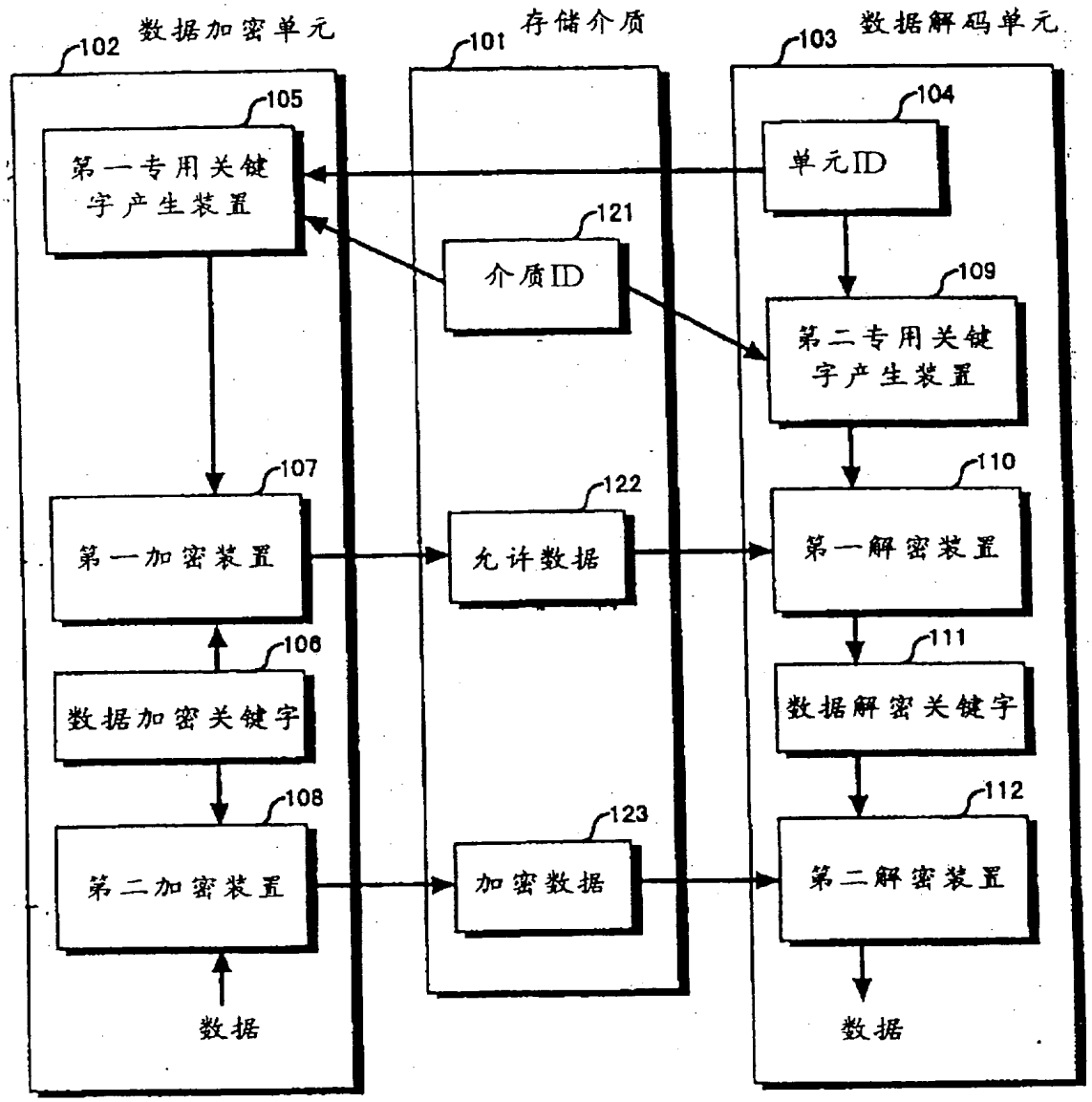


图 10（A）

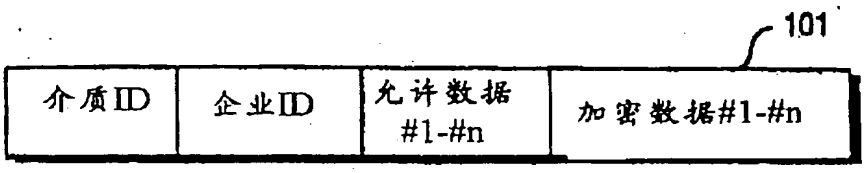


图 10（B）

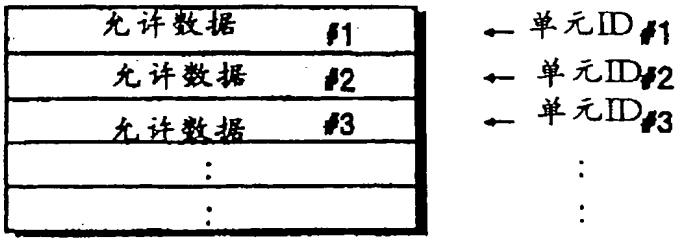


图 11

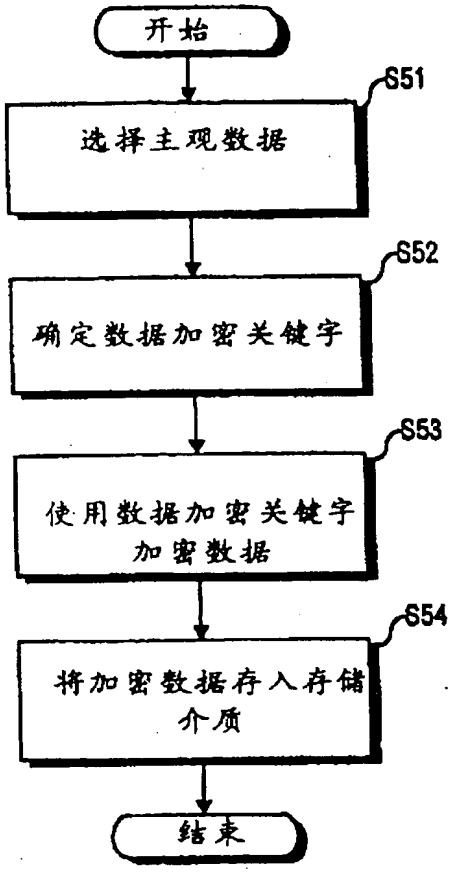


图 12

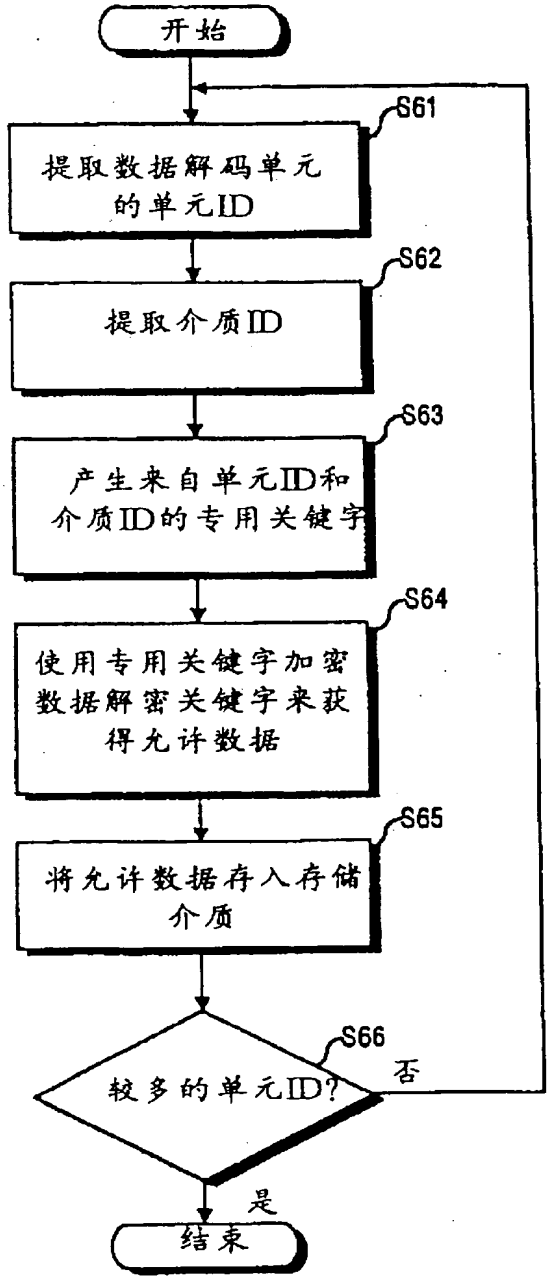
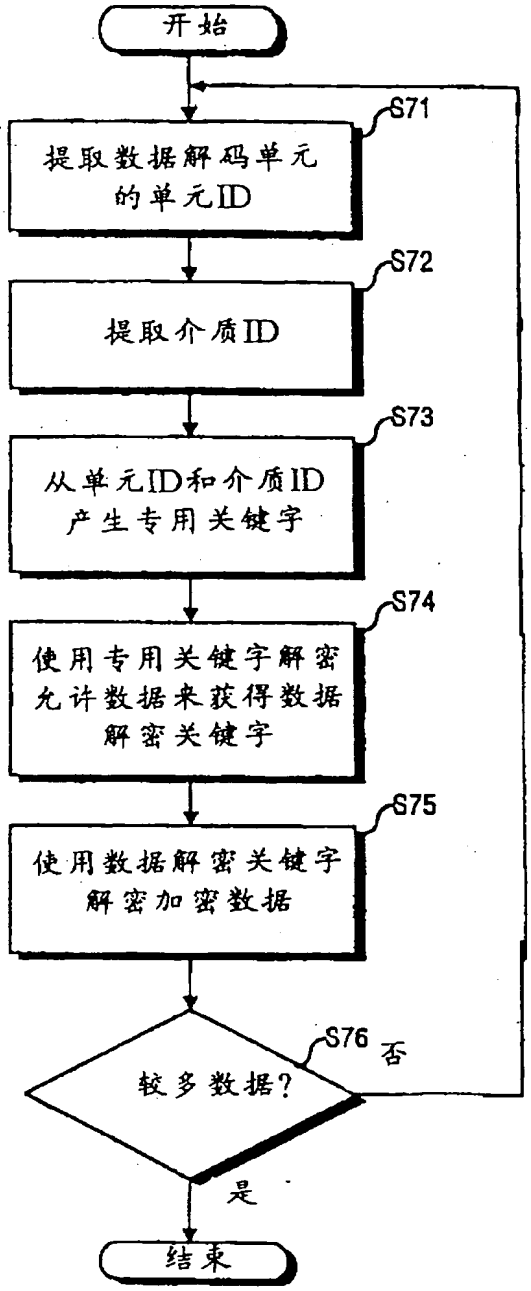


图 13



OA阶段特殊要求

（没有包含案卷和客户的一般性要求）

CPEL0350682P 2005年7月8日

【申请人OA特殊要求】
除分案外，如客户无特殊要求，新申请输入时不用此码，请用JP004054。

本申请之申请人为夏普公司，在转达OA时一定要提供comments供他们考虑。其对转达和答复OA另有许多特殊要求，详见该公司(JP000618)03年4月16日指示及其中译文。